

Confidenziale

Autorità Garante per la protezione dei dati personali
Piazza di Monte Citorio n. 121
00186 ROMA

Dipartimento Comunicazioni e Reti Telematiche

Rif: DCRT/GP/125145

Data: 9 Novembre 2018

Egregi Sig.ri,

Oggetto: Invio di chiarimenti a seguito della richiesta di informazioni dell'11 maggio 2018

Vi scrivo per conto di Facebook Ireland Limited ("**Facebook Ireland**") per quanto riguarda la vostra richiesta di informazioni ricevuta venerdì 11 maggio 2018 (la "**Richiesta**") e la vostra ulteriore richiesta di informazioni inviata il 26 ottobre 2018 relativa al nostro strumento *Ballot* (i.e. Candidati) ("**Ulteriore Richiesta**"). Abbiamo risposto alla Richiesta con tre comunicazioni datate 21 maggio, 13 e 15 giugno 2018 (collettivamente, la "**Risposta**"). Con la presente rispondiamo alle domande della Ulteriore Richiesta e, nella speranza sia di vostra utilità, forniamo ulteriori informazioni rilevanti per la Richiesta.

Al fine di evitare fraintendimenti, Facebook Ireland rimanda alle informazioni e alle argomentazioni espresse in precedenza nella Risposta, che quindi non sono riproposte nella presente comunicazione.

Ci auspichiamo che le informazioni contenute nella presente risposta siano mantenute strettamente confidenziali. Chiediamo rispettosamente la possibilità di integrare o modificare la nostra risposta, se necessario. Facebook Ireland chiede inoltre rispettosamente che tali informazioni siano protette dalla divulgazione e che siano mantenute riservate ai sensi di tutte le leggi applicabili in materia di libertà di informazione. Facebook Ireland richiede inoltre di avvisare la sottoscritta e di dare alla stessa l'opportunità di essere ascoltata nel caso in cui decidiate di divulgare qualsiasi informazione fornita da Facebook Ireland.

Fatte salve le questioni generali sopra indicate, condividiamo con voi le informazioni riportate di seguito, che sono principalmente pertinenti alle domande da (a) a (d) della Richiesta, relative alla questione Cambridge Analytica e alle domande da (h) a (j) della Richiesta, relative all'accesso ai dati degli utenti Facebook da parte di terzi. Non esitate a contattarci se avete ulteriori domande o desiderate chiarimenti su qualsiasi punto.

I. Legge applicabile e foro competente

In via preliminare, ribadiamo la nostra posizione secondo cui Facebook Ireland è l'unico titolare del trattamento per tutti gli utenti UE del servizio Facebook, compresi gli utenti italiani.

Forniamo la presente Risposta su base volontaria e fermo restando che prima dell'entrata in vigore del Regolamento UE 2016/679 - "**GDPR**" - il funzionamento del servizio Facebook in Europa era disciplinato dalle leggi irlandesi sulla protezione dei dati personali ed era soggetto alla regolamentazione dell'*Irish Data Protection Commissioner* ("**IDPC**"). Questo comprenderebbe tutte le questioni menzionate nella Richiesta relative a fatti e circostanze verificatisi prima del 25 maggio 2018.

Dall'entrata in vigore del GDPR, ai sensi dell'articolo 56, paragrafo 1, l'IDPC è l'autorità di controllo capofila per quanto riguarda il servizio Facebook nell'UE. Se codesta Autorità avesse qualche preoccupazione in relazione al trattamento transfrontaliero effettuato da Facebook Ireland nell'ambito del GDPR, dovrebbe fare riferimento all'IDPC come nostro "unico interlocutore" su tali questioni ai sensi delle disposizioni dell'articolo 56, paragrafo 6.

Il concetto di autorità di controllo capofila che agisce in qualità di unico interlocutore per quanto riguarda il trattamento transfrontaliero rappresenta uno dei pilastri del GDPR. Essa mira a conseguire l'uniformità e a creare certezza nell'interpretazione e nell'applicazione della normativa europea in materia di protezione dei dati personali. Qualsiasi tentativo di eludere il ruolo e la competenza dell'autorità di controllo capofila non solo costituirebbe una violazione dell'articolo 56, ma significherebbe vanificare gli sforzi del GDPR per eliminare questa incertezza e incoerenza. Questi concetti fondamentali sono, ad esempio, riconosciuti nel considerando 7 del GDPR, che afferma che *"la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche"*, e nel considerando 13 del GDPR, che rileva che *"e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici"*.

In questo contesto, la presente Risposta è pertanto fornita su base volontaria, fatti salvi i nostri diritti rispetto a giurisdizione e legge applicabile.

II. Cambridge Analytica

Come indicato nelle nostre comunicazioni del 13 e 15 giugno 2018, sebbene l'applicazione del Dr. Kogan, che è diventata nota come "thisisyourdigitallife", potrebbe aver avuto accesso ai dati degli utenti Facebook in tutto il mondo, le prove attualmente a nostra disposizione indicano che il Dr. Kogan ha condiviso tali dati solo con SCL/Cambridge Analytica relativamente agli utenti Facebook situati negli Stati Uniti.

A tutt'oggi non siamo a conoscenza di alcuna prova che suggerisca che il Dr. Kogan abbia fornito a Cambridge Analytica o SCL dati relativi agli utenti Facebook situati nell'UE¹, né tanto meno in Italia. In questo contesto, non rileviamo come la questione Cambridge Analytica possa avere implicazioni significative in termini di protezione dei dati o di privacy per gli utenti Facebook situati in Italia.

III. Accesso ai dati degli utenti Facebook da parte di terzi

A. Ruolo di Facebook come intermediario

La piattaforma Facebook ("**Piattaforma**") è una piattaforma per la condivisione - la sua missione è quella di dare alle persone il potere di costruire una comunità e, in ultima analisi, di avvicinare il mondo. Le persone si uniscono e usano Facebook specificamente per restare in contatto con amici e familiari condividendo informazioni, per scoprire cosa sta succedendo nel mondo e per condividere ed esprimere ciò che conta per loro.

In questo contesto, sebbene abbia sempre cercato di educare ed informare i propri utenti sul funzionamento della Piattaforma, è importante notare che il ruolo di Facebook Ireland nella condivisione dei dati sulla Piattaforma (inclusa la condivisione dei dati da utente ad applicazione) è quello di un intermediario online: facilita le scelte di condivisione dei dati liberamente effettuate dagli utenti in relazione ai dati che controllano, coerentemente con il loro diritto alla libertà di parola

¹ Una considerazione che a quanto ci risulta è stata rilevante, ad esempio, per la decisione dell'autorità spagnola per la protezione dei dati personali di chiudere le rispettive indagini su questioni relative a Cambridge Analytica senza emettere alcuna sanzione nei confronti di Facebook Ireland.

e con l'imperativo di politica pubblica di aumentare la libera circolazione dei dati (imperativo che è stato espressamente riconosciuto nella precedente direttiva 95/46/UE sul trattamento dei dati personali e che è stato ora confermato dal GDPR²).

Durante il periodo in cui l'applicazione del Dr. Kogan operava sulla Piattaforma, la scelta di cosa e quanto condividere utilizzando i servizi tecnici contenuti nella Piattaforma è stata, in linea generale, una scelta degli utenti, non di Facebook Ireland. Gli utenti di Facebook Ireland erano chiaramente informati di come i loro dati potevano essere condivisi con le applicazioni e di cosa potevano fare per esercitare un controllo su questo processo³. Strumenti adeguati sono stati forniti attraverso i vari controlli sulla privacy a disposizione degli utenti della Piattaforma. Tra questi figurano i seguenti (collettivamente denominati "**Controlli sulla Privacy**", come precedentemente riassunti nella nostra risposta alla domanda (a) nella nostra comunicazione del 13 giugno 2018):

- Gli utenti hanno deciso quali informazioni volevano condividere su Facebook in primo luogo;
- Hanno deciso chi volevano come pubblico per qualsiasi informazione che non faceva parte del loro profilo pubblico, ad esempio limitando il pubblico al solo utente o a un gruppo personalizzato di contatti selezionati piuttosto che a tutti gli amici;
- Potevano scegliere di condividere le informazioni con tutti i loro amici, ma limitare la possibilità per le applicazioni dei loro amici di accedere a tali informazioni attraverso le scelte dettagliate offerte nelle impostazioni Apps Usate da Altri; oppure
- Potevano scegliere di condividere le informazioni con i loro amici, ma bloccare completamente l'accesso di qualsiasi applicazione a tali informazioni tramite l'impostazione *Platform Opt-Out*.

Evidenziamo le seguenti caratteristiche relative alla capacità di condivisione dei dati da utente ad applicazione che Facebook ha messo a disposizione degli utenti:

(1) Facebook Ireland non ha ricevuto alcun pagamento a seguito della condivisione dei dati degli utenti con applicazioni di terze parti;

(2) La condivisione dei dati degli utenti con le applicazioni di terze parti che utilizzavano Facebook Login si è sempre verificata per iniziativa degli utenti che stavano cercando di installare l'applicazione in questione: è stata la *loro* decisione di condividere i dati con l'applicazione che ha portato la stessa ad ottenere i dati;

(3) il processo con cui gli utenti condividono i dati con le applicazioni è stato in effetti una transazione privata tra utente e applicazione, agevolata da Facebook Ireland;

(4) Il ruolo di Facebook Ireland nell'ambito di tale operazione è sempre stato quello di un intermediario online: tecnicamente Facebook Ireland ha facilitato le decisioni di condivisione dei dati effettuate attivamente dai propri utenti. In effetti, il ruolo di Facebook Ireland era quello di rispondere, su base automatizzata, ai comandi di condivisione dei dati impartiti dagli utenti in relazione ai dati che essi stessi controllavano (che nella V1 della Piattaforma includevano alcuni dati che gli amici degli utenti avevano scelto di condividere con loro su Facebook, fatte salve le scelte sulla privacy effettuate da tali amici come risulta dai rispettivi Controlli sulla Privacy); e

(5) Facebook Ireland ha potuto fornire tali mezzi tecnici solo nei casi in cui la trasmissione dei dati all'applicazione sia stata effettuata su esplicita indicazione dell'utente che ha installato

² Si veda, ad esempio, considerando 3 e articolo 1, paragrafo 2, della direttiva 95/46/UE e articolo 20 del GDPR.

³ Si vedano le risposte alle domande (b), (c) e (i) della Richiesta nella nostra comunicazione del 15 giugno 2018.

l'applicazione e, in base alla V1, sia stata altrimenti autorizzata da qualsiasi amico di tale utente in conformità con i rispettivi Controlli sulla Privacy.

La raccolta di dati tramite Facebook Login da parte di queste applicazioni di terze parti indipendenti è sempre stata distinta dalle attività di raccolta dati di Facebook Ireland. È stato lo sviluppatore di applicazioni di terze parti che ha richiesto agli utenti l'autorizzazione a raccogliere i dati e lo ha fatto in base: (i) agli obblighi contrattuali esistenti nei confronti dei propri utenti ai sensi dei termini e delle condizioni che aveva stipulato con tali utenti; e (ii) agli obblighi di legge ai quali era soggetto ai sensi della legislazione applicabile in materia di protezione dei dati personali in qualità di titolare autonomo del trattamento dei dati personali. La responsabilità e l'onere giuridico di controllare l'uso dei dati da parte di questi terzi spetta alle autorità di controllo competenti piuttosto che a Facebook Ireland. Concludere altrimenti pregiudicherebbe il concetto di titolare del trattamento dei dati e sarebbe inoltre contrario ai principi sanciti dalla normativa dell'Unione Europea a tutela degli intermediari online.

Tuttavia, con la volontà di andare oltre le proprie responsabilità legali al fine di fornire ulteriori garanzie ai propri utenti, Facebook Ireland ha imposto obblighi contrattuali alle applicazioni di terze parti che utilizzano la sua Piattaforma attraverso le sue Condizioni e la sua Politica della Piattaforma. Tra le altre cose, questo ha richiesto alle applicazioni di terze parti di mettere in atto politiche appropriate e di ottemperare alle leggi sulla privacy applicabili⁴. Gli sviluppatori dovevano inoltre osservare standard appropriati e rispettare il divieto di Facebook Ireland di vendere o concedere in licenza i dati di utenti a cui utenti hanno avuto accesso dalla Piattaforma di Facebook Ireland e di condividere i dati di utenti Facebook con qualsiasi rete pubblicitaria, data broker o altro servizio legato alla pubblicità o alla monetizzazione.

B. Monitoraggio e applicazione

C. La Piattaforma e la supervisione da parte delle autorità di controllo

Facebook Ireland ha un'esperienza di grande impegno, costruttivo e cooperativo, con IDPC in qualità di autorità di controllo capofila. Questo comprende l'ampio e dettagliato lavoro di audit che l'IDPC ha svolto nel 2011 e nel 2012 per valutare la conformità di Facebook alle leggi applicabili sulla privacy (che ha portato alla Relazione di Audit 2011⁶ e alla Relazione di Re-Audit 2012⁷). L'IDPC ha elogiato Facebook Ireland nel corso delle proprie attività di audit 2011/2012 per l'approccio positivo e l'impegno di Facebook Ireland a rispettare i diritti alla privacy dei propri utenti⁸.

A seguito del processo di audit 2011/2012, l'IDPC è stato chiaro nel determinare che l'audit e le raccomandazioni che ne sono scaturite non hanno constatato la mancata conformità delle pratiche di Facebook Ireland rispetto alla legge europea sulla protezione dei dati (così come recepita dalla legge irlandese sulla protezione dei dati⁹). In effetti, l'IDPC ha formulato le proprie raccomandazioni come raccomandazioni di migliore prassi ('best practice'), vale a dire al di là della conformità giuridica. Nel giungere alle sue conclusioni sulla condivisione dei dati da utente ad applicazione sulla Piattaforma, l'IDPC è stato informato mediante dettagliate relazioni tecniche redatte da un esperto indipendente incaricato dall'IDPC, che comprendevano una spiegazione del funzionamento della Piattaforma e di come gli utenti potevano consentire la condivisione dei dati degli amici con applicazioni di terze parti. Queste relazioni tecniche, elaborate a seguito di un ampio esame diretto dei sistemi Facebook, sono state rese pubbliche insieme alle Relazioni di Audit dell'IDPC e hanno corroborato le raccomandazioni sulle migliori prassi formulate dall'IDPC. L'aspetto importante è che l'audit IDPC, il funzionamento della Piattaforma ed i risultati ottenuti sono stati caratterizzati da una notevole trasparenza.

Nell'ambito del processo di audit 2011/2012, l'IDPC ha preso in particolare considerazione l'utilizzo di applicazioni di terzi sulla Piattaforma. Un lavoro analogo è stato svolto anche da altre autorità di controllo, in particolare dal *Canadian Office of the Privacy Commissioner*, dalla *US Federal Trade Commission* ("FTC") e dalle autorità nordiche e tedesche per la protezione dei dati. L'IDPC ha osservato che l'FTC ha esaminato il funzionamento delle applicazioni di terzi sulla Piattaforma e la portata dei dati ai quali le applicazioni di terzi possono cercare di accedere.¹⁰ L'IDPC ha inoltre esaminato una serie di questioni specifiche sollevate nei reclami indirizzati all'Ufficio dal gruppo "Europe-versus-Facebook", dal Consiglio Norvegese dei Consumatori e da un certo numero di persone fisiche. Questi reclami includevano il suggerimento (errato) che *"gli utenti Facebook non sono a conoscenza del fatto che se un loro amico di Facebook installa un'applicazione, tale applicazione ha la possibilità di accedere alle informazioni di base del profilo di quell'amico dell'utente, come foto e nome"*. Queste parti sono state in grado di sollevare questioni con l'IDPC sulle sue opinioni iniziali e sulle risposte pubblicate da Facebook Ireland.

L'IDPC ha dichiarato che il funzionamento delle applicazioni di terze parti è stato uno dei punti focali del lavoro di audit¹¹ e alla luce dei reclami ricevuti in merito alla questione ha esaminato in particolare come garantire che gli utenti siano in grado di effettuare scelte informate sui dati che gli amici possono condividere con le applicazioni di terze parti¹². L'IDPC ha rilevato che gli utenti potevano già fare tale scelta utilizzando i loro Controlli sulla Privacy, ma ha raccomandato a

⁶ <https://www.dataprotection.ie/documents/facebook%20report/linal%20report/report.pdf>

⁷ https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf

⁸ IDPC 2011 Relazione di Audit, p 3

⁹ IDPC 2011 Relazione di Audit, p 4

¹⁰ Cfr. FTC 29 novembre 2011 Reclamo, paragrafo 9. Questo ha osservato: "Facebook ha progettato la sua Piattaforma in modo tale che le Applicazioni della Piattaforma possano accedere alle informazioni sul profilo utente in due istanze principali. In primo luogo, le Applicazioni della Piattaforma che un utente autorizza possono accedere alle informazioni sul profilo dell'utente. In secondo luogo, se l'"Amico" di un utente autorizza un'Applicazione della Piattaforma, tale applicazione può accedere ad alcune delle informazioni del profilo dell'utente, anche se l'utente non ha autorizzato tale Applicazione. Ad esempio, se un utente autorizza un'Applicazione della piattaforma che fornisce promemoria sui compleanni degli Amici, tale applicazione potrebbe accedere, tra le altre cose, ai compleanni degli Amici dell'utente, anche se questi Amici non hanno mai autorizzato l'applicazione". Vedere anche Relazione di Audit IDPC 2011, pagina 87.

¹¹ IDPC 2012 Relazione di Rc-Audit, pagina 29

¹² IDPC 2012 Relazione di Re-Audit, pagina 31

Facebook Ireland di migliorare la scelta e il controllo granulare in quest'area¹³. A seguito di ulteriori modifiche apportate da Facebook Ireland, l>IDPC ha successivamente rilevato la positiva adozione delle proprie raccomandazioni sulle migliori prassi, anche nei settori chiave della trasparenza, del controllo degli utenti e della sicurezza dei dati¹⁴.

Per il resto facciamo riferimento e rimandiamo, in particolare, alle seguenti sezioni delle Relazioni di Audit IDPC:

- Sezione 3.1 della Relazione di Audit 2011 - *Privacy Policy / Data Use Policy* - L>IDPC ha registrato risposte soddisfacenti da parte di Facebook Ireland per quanto riguarda la semplificazione e la crescente evidenza della sua Privacy Policy. Infatti, l'ambizione di IDPC era di garantire *"una maggiore capacità degli utenti di fare le proprie scelte informate sulla base delle informazioni disponibili"*¹⁵. Nella Relazione di Re-Audit 2012, l>IDPC ha registrato che Facebook Ireland ha apportato modifiche alla comunicazione "appena in tempo" di informazioni agli utenti, il che significa che *"quando un utente sta effettuando una scelta o è invitato a fare una scelta su come desidera che i suoi dati personali siano utilizzati, gli siano presentate in quel momento informazioni pertinenti e comprensibili su cui basare la propria scelta"*¹⁶. Per una trattazione completa si rimanda alla sezione 3.1 della Relazione di Audit 2011 e alle pagine 13-15 della Relazione di Re-Audit 2012.
- Sezione 3.6 della Relazione di Audit 2011 - Applicazioni di terzi - L>IDPC ha registrato nella sua Relazione di Audit 2012 che il funzionamento delle applicazioni di terzi *"è stato un punto focale significativo del nostro Audit di dicembre [2011]"*¹⁷ e che Facebook Ireland ha attuato in maniera soddisfacente la maggior parte delle raccomandazioni dell>IDPC. Una discussione completa si trova alla sezione 3.6 della Relazione di Audit 2011 e alle pagine 33-34 della Relazione di Re-Audit 2012.
- Le principali raccomandazioni e conclusioni delle Relazioni di Audit IDPC sono ripetute di seguito per comodità di riferimento.
 - Raccomandazione 1: attraverso informazioni e strumenti adeguati gli utenti devono essere messi in grado di prendere decisioni informate quando concedono l'accesso ai loro dati da parte di applicazioni di terzi. (L>IDPC ha preso nota in particolare che Facebook ha fornito informazioni chiare prima dell'installazione dell'applicazione del Dr. Kogan, commentando: *"riteniamo che gli sviluppi di cui sopra abbiano fornito agli utenti un mezzo per esercitare una scelta basata su informazioni chiare prima di decidere se installare un'applicazione"*).¹⁸
 - Raccomandazione 4: Facebook dovrebbe verificare se i link alle politiche sulla privacy delle applicazioni di terze parti siano attivi. *"Siamo quindi lieti che FB-I ha adottato questa raccomandazione e ha presentato uno strumento interno che garantisce che tutte le applicazioni disponibili sul sito abbiano un link attivo alla politica sulla privacy"*.¹⁹
 - *"Conclusione: Abbiamo verificato che non era possibile per un'applicazione accedere ai dati personali oltre a quelli a cui un individuo dà il proprio consenso o che ha abilitato tramite le relative impostazioni"*.²⁰

¹³ IDPC 2012 Relazione di Re-Audit, pagina 31

¹⁴ 2012 Relazione Annuale, pagina 3 and pagina 19.

https://www.dataprotection.ie/documents/annualreports/Annual_Report_2012.pdf

¹⁵ IDPC 2011 Relazione di Audit, pagina 42

¹⁶ IDPC 2012 Relazione di Re-Audit, pagina 14

¹⁷ IDPC 2012 Relazione di Re-Audit, pagina 29

¹⁸ IDPC 2012 Relazione di Re-Audit, pagina 30

¹⁹ IDPC 2012 Relazione di Re-Audit, pagina 30

²⁰ IDPC 2012 Relazione di Re-Audit, pagina 30

- Sezione 3.9 della Relazione di Audit 2011 - Sicurezza dei dati - Nella Relazione di Audit 2011, l>IDPC ha rilevato di aver dedicato "una particolare attenzione durante l'audit alla valutazione delle questioni di sicurezza".²¹ In effetti, l>IDPC ha riconosciuto che anche Facebook *"pone un'enorme e costante attenzione alla protezione e alla sicurezza dei dati degli utenti"*.²² Una discussione completa si trova al paragrafo 3.9 della Relazione di Audit 2011 e alle pagine 39-41 della Relazione di Re-Audit 2012.

E' sorprendente che codesta autorità sembri indicare, circa sette anni dopo, che ora nutre preoccupazioni riguardo al funzionamento della Piattaforma dal 2011/2012 in avanti. Ciò è tanto più vero se si considera che: (a) l>IDPC non ha condotto la sua revisione in maniera isolata e si è attivamente consultato con i membri del Gruppo di lavoro UE Articolo 29 (*Working Party Article 29*); e (b) nel 2011 sono state pubblicate dall>IDPC informazioni dettagliate sulla condivisione dei dati da utente ad applicazione sulla Piattaforma (comprese le informazioni sulla portata dei dati a cui le applicazioni terze parti potrebbero chiedere di accedere).

Nella sua Relazione Annuale 2012, l>IDPC ha riassunto i risultati delle Relazioni di Audit IDPC come segue (enfasi aggiunta):

"Nel 2011 è stato condotto un importante audit su Facebook Ireland (FB-I), la cui relazione è stata pubblicata nel dicembre 2011. A seguito dell'audit, FB-I ha accettato un'ampia gamma di migliorie in materia di "migliori prassi", con un esame formale dei progressi che si svolgerà nel luglio 2012.

Nel settembre 2012, il Dipartimento ha pubblicato i risultati della nostra revisione dell'implementazione da parte di Facebook Ireland (FB-I) delle raccomandazioni formulate nel nostro Audit.

Dalla Revisione è emerso che la grande maggioranza delle raccomandazioni è stata pienamente attuata in modo soddisfacente, in particolare nelle seguenti aree:

- *L'offerta di una maggiore trasparenza per l'utente nel modo in cui vengono gestiti i suoi dati,*
- *L'offerta di un maggiore controllo dell'utente sulle impostazioni,*
- *L'attuazione di periodi di conservazione chiari per la cancellazione dei dati personali o una maggiore capacità di cancellazione dell'utente,*
- *Il rafforzamento del diritto dell'utente ad avere un accesso immediato ai propri dati personali e la capacità di FB-I di garantire una rigorosa valutazione del rispetto dei requisiti irlandesi e dell'UE in materia di protezione dei dati.*

Le raccomandazioni che all'epoca non erano state attuate da FB-I sono state evidenziate con un chiaro programma di attuazione. È stato fissato un termine di 4 settimane per la conclusione soddisfacente di tali questioni e FB-I ha compiuto progressi soddisfacenti nel periodo di quattro settimane. L'Ufficio continua a mantenere un dialogo costante con FB-I sulle implicazioni per la protezione dei dati di tutti i nuovi servizi man mano che questi vengono introdotti.

Nel corso dell'anno l'Ufficio si è ampiamente consultato con i colleghi di altre Autorità preposte alla Protezione dei Dati su questioni che sono emerse nell'ambito del processo di Audit e su questioni che hanno destato preoccupazione o interesse per i colleghi in generale. Nella misura in cui ciò è stato possibile, abbiamo cercato di tenere conto di tali questioni e di ottenere risultati soddisfacenti. Ciò è emerso dal nostro riconoscimento del fatto

²¹ IDPC 2011 Relazione di Audit, pagina 107

²² IDPC 2011 Relazione di Audit, pagina 108

che, sebbene fossimo responsabili della supervisione di Facebook in Europa attraverso la sua società irlandese, era necessario consultare pienamente e tenere conto delle opinioni dei colleghi i cui cittadini nutrono preoccupazioni su alcuni aspetti legati all'utilizzo dei loro dati personali da parte di Facebook".

Il risultato di queste conclusioni è che, alla fine del processo di audit, l'IDPC ha considerato l'approccio di Facebook Ireland alla trasparenza, al controllo e alla sicurezza dei dati sulla Piattaforma come giuridicamente inoppugnabile. Come è ragionevole attendersi, Facebook Ireland si è basata su queste conclusioni andando avanti, come aveva il diritto di fare.

In questo contesto è importante considerare che, al fine di garantire la libera circolazione dei dati in Europa, che era a sua volta un pilastro fondamentale della direttiva (e ora del GDPR), le autorità di controllo dovrebbero sforzarsi di svolgere i loro compiti di regolamentazione in modo altamente concorde. Qualsiasi altro approccio all'attuazione della normativa all'interno dell'UE rischia di avere un effetto limitante significativo sulla realizzazione della mobilità dei dati in Europa ed è inoltre scorretto nei confronti dei titolari del trattamento che hanno il diritto di presumere che le autorità di controllo dell'UE applicheranno in generale le leggi sulla protezione dei dati in modo coerente e uniforme in tutta l'UE.

Per completezza notiamo che, come saprete, l'ufficio del *UK Information Commissioner* ("ICO") ha recentemente emesso una sanzione nei confronti di Facebook in relazione alla questione Cambridge Analytica. Facebook Ireland sta attualmente riesaminando la decisione dell'ICO e avrebbe il diritto di impugnare tale sanzione dinanzi al tribunale "English Information" sulla base del fatto che essa è gravemente viziata da molteplici e gravi errori di fatto e di diritto compreso, non da ultimo, il fatto che l'ICO non ha tenuto conto delle conclusioni raggiunte dall'IDPC (in consultazione con altre autorità europee per la protezione dei dati personali) nel contesto della sua revisione dell'approccio di Facebook Ireland allo scambio di dati da utente ad applicazione sopra illustrato.

IV. L'ulteriore Richiesta

Come punto di partenza per quanto riguarda le questioni sollevate nella Ulteriore Richiesta, è necessario chiarire lo scopo del nostro strumento Ballot, nonché le iniziative specifiche che si sono svolte nell'ambito delle elezioni italiane del 2018. Questo perché dalla sintesi fornita nella comunicazione di codesta autorità contenente l'Ulteriore Richiesta sembra che ci possa essere una certa confusione al riguardo.

Ballot era uno strumento messo a disposizione degli utenti italiani per facilitare l'accesso alle informazioni sui candidati nel loro distretto elettorale. Oltre a facilitare l'accesso alle informazioni sui candidati - e a seguito della collaborazione con il Ministero dell'Interno, la Presidenza del Consiglio dei Ministri e varie altre organizzazioni e candidati in tutto il paese - Ballot includeva anche un video tutorial per educare gli utenti sui nuovi requisiti di voto e sulle nuove leggi elettorali che venivano introdotte in Italia.

Lo strumento è stato reso disponibile per l'utilizzo su base "opt-in", il che significa che era del tutto facoltativo per gli utenti decidere se usufruire o meno con il prodotto.

Desideriamo sottolineare che Ballot è stato lanciato esclusivamente come strumento di educazione civica e di coinvolgimento, come parte del nostro impegno a sostegno di una comunità informata e civicamente impegnata sulla nostra piattaforma. Lo strumento non è stato in alcun modo lanciato per il "monitoraggio del comportamento elettorale", contrariamente a quanto dichiarato nella vostra comunicazione. Infatti lo strumento è stato appositamente progettato per **non** registrare informazioni su come i singoli utenti possono aver votato nelle elezioni.

Separatamente, e come iniziativa distinta dal nostro prodotto Ballot, come ulteriore parte del nostro impegno a sostenere l'impegno civico sulla nostra piattaforma per le elezioni del 2018, abbiamo

pubblicato un promemoria del giorno delle elezioni nelle Notizie degli utenti italiani. Questo promemoria ha fornito agli utenti informazioni su come e dove votare e ha anche dato loro la possibilità di condividere il fatto che avevano votato. Abbiamo anche reso disponibili i risultati elettorali su Facebook dopo la chiusura dei sondaggi e, dopo la formazione del nuovo governo, abbiamo fornito una notifica in-app che permetteva agli utenti di scoprire chi erano i loro attuali e nuovi rappresentanti.

In questo contesto, le domande specifiche sollevate nell'Ulteriore Richiesta sono di seguito considerate nel dettaglio:

(a) Quale trattamento sia stato effettuato rispetto ai dati personali acquisiti con i file di log relativi all'accesso dei singoli utenti ai profili dei candidati e alla loro eventuale manifestazione di aver votato?

Come spiegato nella nostra risposta del 21 maggio 2018, abbiamo ottenuto dei log di base delle azioni degli utenti che hanno scelto di utilizzare Ballot. Queste informazioni sono state utilizzate solo allo scopo di generare metriche di ingaggio aggregate - cioè metriche generalizzate che forniscono una panoramica su come gli utenti di Facebook nel loro complesso si sono confrontati con il prodotto, e non un'analisi su come specifici individui possono aver utilizzato il prodotto. Queste metriche aggregate ci hanno aiutato a comprendere come il prodotto veniva utilizzato e come poteva essere migliorato per renderlo più utile in generale per gli utenti nelle future elezioni, sia in Italia che in altri paesi. I dati di log sottostanti utilizzati per creare queste metriche aggregate sono stati cancellati dopo 90 giorni.

Per quanto riguarda la seconda parte della vostra domanda - vale a dire quale trattamento sia stato effettuato rispetto ai dati personali contenuti nei post degli utenti che manifestavano di aver votato - non abbiamo monitorato il contenuto dei post che gli utenti hanno scelto di pubblicare per valutare o comprendere in alcun modo le loro decisioni di voto. Lo scopo dei messaggi che abbiamo inviato agli utenti era semplicemente quello di incoraggiare l'impegno civico sulla nostra piattaforma. Come per tutti i loro post, gli utenti possono vedere ciò che hanno postato in precedenza e cancellarlo in qualsiasi momento, anche attraverso il loro Registro Attività.²³

(b) A quale finalità tale trattamento rispondeva?

Si veda la nostra risposta alla precedente lettera (a).

(c) Di quali dati era costituito l'"indirizzo postale" (l'indirizzo nella sua interezza o solo il CAP)?

Se un utente desiderava utilizzare il prodotto Ballot, poteva inserire il proprio indirizzo postale completo. Ciò era necessario per garantire che la rispettiva circoscrizione elettorale fosse correttamente identificata e che venissero mostrate all'utente le corrette informazioni sul candidato - ad esempio, la semplice indicazione di un codice postale sarebbe stata insufficiente per accertare in modo affidabile la circoscrizione elettorale di un utente. Come spiegato nella nostra comunicazione precedente, agli utenti è stato dato pieno controllo sulle informazioni circa l'indirizzo che hanno scelto di fornire in questo modo (supponendo in primo luogo che avessero scelto di utilizzare il prodotto Ballot). Gli utenti potevano saltare l'inserimento o, una volta venuti a conoscenza dei loro candidati locali, potevano rimuoverlo o modificarlo.

d) Quali informazioni sono state fornite agli interessati in merito ai predetti trattamenti?

Come spiegato nella nostra precedente risposta, la nostra Data Policy ha spiegato agli utenti quali informazioni abbiamo raccolto e come le abbiamo utilizzate. Ad esempio, la Data Policy in vigore al momento delle elezioni del 2018 prevedeva quanto segue:

²³ <https://www.facebook.com/help/289066827791446>

I. Che tipo di informazioni raccogliamo?

A seconda dei Servizi che utilizzate, raccogliamo diversi tipi di informazioni da voi o su di voi.

- **Cose che fai e informazioni che fornisci.** Raccogliamo il contenuto e le altre informazioni fornite dall'utente quando utilizza i nostri Servizi, anche quando si registra un account, crea o condivide, e invia messaggi o comunica con altri. Questo può includere informazioni sul contenuto fornito dall'utente, come la localizzazione di una foto o la data di creazione di un file. Raccogliamo anche informazioni su come gli utenti utilizzano i nostri Servizi, come ad esempio i tipi di contenuti che visualizzano o utilizzano o la frequenza e la durata delle loro attività.

[...]

II. Come utilizziamo queste informazioni?

Siamo motivati a creare esperienze coinvolgenti e personalizzate per le persone. Usiamo tutte le informazioni che abbiamo per aiutarci a fornire e supportare i nostri Servizi. Ecco come:

- **Fornire, migliorare e sviluppare i Servizi.** Siamo in grado di fornire i nostri Servizi, personalizzare i contenuti e dare suggerimenti per voi utilizzando queste informazioni per capire come usate e interagite con i nostri Servizi e con le persone o cose a cui siete connessi e interessati dentro e fuori dai nostri Servizi. [...] Effettuiamo indagini e ricerche, testiamo le funzionalità in fase di sviluppo e analizziamo le informazioni di cui disponiamo per valutare e migliorare prodotti e servizi, sviluppare nuovi prodotti o funzionalità, condurre audit e attività di risoluzione dei problemi.

[...]

III. Come vengono condivise queste informazioni?

Condivisione sui nostri Servizi

Le persone utilizzano i nostri Servizi per connettersi e condividere con gli altri. Lo rendiamo possibile condividendo le tue informazioni nei seguenti modi:

- **Le persone con cui condividi e con cui comunichi.** Quando condividi e comunichi utilizzando i nostri Servizi, scegli il pubblico che può vedere ciò che condividi. Ad esempio, quando pubblichi su Facebook, selezioni il pubblico per il post, come un gruppo personalizzato di individui, tutti i tuoi Amici o membri di un Gruppo. Allo stesso modo, quando usi Messenger, scegli anche le persone a cui inviare foto o messaggi. Le informazioni pubbliche sono tutte le informazioni che condividi con un pubblico, così come le informazioni del tuo Profilo Pubblico, o i contenuti che condividi su una pagina Facebook o un altro forum pubblico. Le informazioni pubbliche sono disponibili a chiunque, dentro o fuori dai nostri Servizi e possono essere visualizzate o accessibili attraverso motori di ricerca online, API e media offline, come ad esempio in TV. In alcuni casi, le persone con cui condividi e con cui comunichi possono scaricare o condividere nuovamente questo contenuto con altri, sia all'interno che all'esterno dei nostri Servizi. Quando commentate un post di un'altra persona o vi piace il loro contenuto su Facebook, quella persona decide il pubblico che può vedere il vostro commento o il mi piace. Se il loro pubblico è pubblico, anche il tuo commento sarà pubblico.

[...]

IV. Come posso gestire o cancellare le informazioni che mi riguardano?

Puoi gestire i contenuti e le informazioni che condividi quando usi Facebook attraverso lo strumento Registro Attività. Puoi anche scaricare le informazioni associate al tuo account Facebook attraverso il nostro strumento Scarica le tue informazioni.

I dati vengono conservati per tutto il tempo necessario per fornire prodotti e servizi a te e ad altri, compresi quelli sopra descritti. Le informazioni associate al tuo account saranno conservate fino alla cancellazione del tuo account, a meno che non siano più necessari per fornire i prodotti e servizi.

Puoi cancellare il tuo account in qualsiasi momento. Quando cancelli il tuo account, cancelliamo le cose che hai postato, come le tue foto e gli aggiornamenti di stato. Se non vuoi cancellare il tuo account, ma vuoi interrompere temporaneamente l'utilizzo di Facebook, puoi disattivare il tuo account. Per ulteriori informazioni su come disattivare o eliminare il tuo account, clicca qui. Tieni presente che le informazioni che altri hanno condiviso su di te non fanno parte del tuo account e non verranno eliminate quando cancellerai il tuo account.

L'attuale Normativa sui dati, da allora aggiornata, è disponibile al seguente link: <https://www.facebook.com/policy.php>.

Come spiegato anche nella nostra risposta precedente, Ballot ha fornito agli utenti specifiche indicazioni inserite nel prodotto stesso e "in tempo reale" che erano mostrate nel momento in cui veniva presentata agli utenti la possibilità di inserire il proprio Indirizzo. Questo includeva istruzioni su come gli utenti potevano modificare o rimuovere queste informazioni in qualsiasi momento, così come un link "Per saperne di più" per quegli utenti che erano interessati a scoprire informazioni più dettagliate sul perché Facebook avesse bisogno del loro indirizzo per Ballot e su come tali informazioni sarebbero state utilizzate. Informazioni simili erano generalmente disponibili anche nel nostro Centro Assistenza.²⁴

e) Cosa si intende con l'espressione "matrici di ingaggio aggregate" (risposta del 21 maggio 2018), fornendo possibilmente degli esempi?

Come spiegato nella nostra risposta alla domanda (a) di cui sopra, le matrici di ingaggio aggregate sono matrici che forniscono una panoramica su come gli utenti Facebook nel loro insieme si rapportano ad un prodotto. **Non** sono una sorta di analisi su come specifici individui possono aver utilizzato il prodotto Ballot. Queste matrici di ingaggio aggregate ci hanno aiutato a comprendere come il prodotto Ballot veniva utilizzato in generale e come poteva essere migliorato per renderlo più utile per gli utenti nelle elezioni future. Ad esempio, abbiamo analizzato la quantità media di tempo dedicato alle diverse caratteristiche del prodotto, come indicatore del fatto che gli utenti in generale trovassero tali caratteristiche utili o interessanti. Questa analisi ci ha permesso di prendere decisioni più ponderate su quali parti del prodotto potrebbero trarre beneficio dai miglioramenti.

f) Con riferimento infine all'espressione utilizzata nelle FAQ "le informazioni che fornisci possono anche essere utilizzate per future funzioni di Facebook", quali sono in dettaglio i dati personali richiesti agli utenti "per future funzioni di Facebook" e quali sono le finalità per le quali possono essere conservati tali dati personali?

²⁴ <https://www.facebook.com/help/299618223782909>

Traduzione di cortesia

Al momento utilizziamo le informazioni sugli indirizzi forniti dagli utenti italiani di Facebook attraverso l'uso di Ballot soltanto ai fini delle funzioni elettorali e governative su Facebook. Le uniche funzioni di questo tipo finora introdotte in Italia che hanno utilizzato tali informazioni sugli indirizzi - se gli utenti hanno scelto di fornirle - sono Ballot e la notifica in-app che è stata rilasciata sul mobile dopo le elezioni del 2018, invitando gli utenti a individuare e seguire i loro nuovi rappresentanti eletti, come spiegato sopra.

Spero che queste informazioni siano utili per rispondere alle domande che avete posto. Non esitate a contattarci se avete bisogno di ulteriori informazioni.

Vi alleghiamo una traduzione italiana di cortesia della presente comunicazione.

Distinti saluti



Head of Data Protection, Facebook Ireland Limited